To: Merritt Baer, Stuart Brotman, Davi Ottenheimer, Ken Rogerson

From: Dev Seth, Ishaan Kumar, Megan Richards

Subject: A Privacy-Centric Contact Tracing Framework

Date: April 26, 2020

Introduction

Contact tracing is the process of identifying and protecting individuals who are at risk of disease contraction because of past contact with infected individuals [1]. In the course of the ongoing COVID-19 pandemic, many countries have used contact tracing and contact testing/isolation as the bedrock of their mitigation strategy [2]. While countries like South Korea and Singapore have demonstrated the public health promise of digital contact tracing, significant privacy and socio-political issues remain [3].

We propose a digital contact tracing framework that guarantees privacy by eliminating the risks associated with invasive identifiers and central storage of sensitive data. Our solution protects individual freedoms without sacrificing the efficacy of contact tracing.

Primary Concerns

We delineate the contact tracing process into three steps:

1. Track Interpersonal Proximity
2. Report Positive Cases
3. Alert Contacts

Privacy issues with steps 1 and 3 are the risks associated with the centralization of data. This includes civil rights issues such as the right to privacy, the ability for individuals to have control over their medical data, and the danger of constant surveillance, which has historically been a slippery slope to the erosion of other fundamental freedoms [4] [5].

The issue with step 2 is a practical one, since most existing app-based solutions rely on individuals to self-report their test results. Pushing the burden of reporting onto individuals reduces the fidelity of the data and opens the door to trolling/misuse.

Tracking Interpersonal Proximity

A contact-tracing application must collect the minimum number of identifiers needed to achieve its objective. Applications like Aarogya Setu (India) use absolute location identifiers like GPS when relative location identifiers like Bluetooth signal strength are equally efficacious [6] [7]. Apps

collecting non-essential or tangentially-relevant identifiers are guilty of *scope creep*, and are more likely to pose a privacy risk.

Our solution uses Bluetooth and ultrasound to track interpersonal proximity. Each user device locally generates a random temporary public key which is updated at 10 minute intervals. This key is not correlated with any personally identifiable information about the user. Each device ambiently broadcasts its key to other devices in range. Devices store detected keys in the app's encrypted memory for future use. Public keys managed without the need for a central server, since every device maintains its own list of contacts. Entries are automatically removed one week after the 14-day incubation period.

Reporting Positive Cases

It is vital for an app-based solution to provide confidence to its users about the authenticity of the alerts that they receive. Self-report systems like Singapore's TraceTogether minimize identification risk with an entirely decentralized data model [8], but are prone to underreporting and face the risk of false claims [9] and trolling. Alternatively, mandatory reporting systems violate individuals' right to control the use of their information, such as in South Korea where reported data was re-identified and used to doxx or harass individuals. [3].

In our model, individuals are given an additional consent form at the time of testing, and can choose to share a QR code generated by the app with the authorities at the testing location. In the event that the user tests positive, the information in this QR code allows the health authorities to establish trusted communication with the user's device and obtain all temporary keys generated on the device for dissemination.

This approach respects informed consent, eliminates the burden of self-reporting, and precludes trolling attempts.

Alerting Those at Risk

For this step, privacy concerns stem from the disruption of the data flow between the healthcare agency, government database, and user.

In our solution, healthcare authorities collect public keys from consenting COVID-positive individuals and publish the keys to a central feed. Individual devices subscribe to this feed and alert the user of a match with a previously received key. Since the keys are not visible to the user and don't contain personally identifying information, a data breach would not compromise user identity, nor would the alerted user know whose positive result generated the match.

Implementation

When the application is first deployed, it should be accompanied by stringent regulations that prevent any third party use of its data, and a clear plan for dismantling the health surveillance apparatus at the end of the pandemic. The code for the application must be open-sourced.

In general, the limitations of contact tracing apps vary across national and societal contexts, influenced by cultural attitudes, levels of testing, smartphone market penetration, app adoption rates, and health-tech infrastructure.

Based on our choice of architecture, we obtain privacy and decentralization by incurring the following limitations:

1. Reliance on unidirectional broadcast of public keys requires additional protection from spoofing attacks.
2. Decentralized data storage curtails the benefits of analytics performed on aggregated data.
3. Offline-only storage relies on device integrity, so lost data cannot be recouped if a device breaks.
4. Relative instead of absolute location identifiers make it harder to geolocate emerging hotspots.

. ■

References

[EK03] K. T. D. Eames and M. J. Keeling. "Contact tracing and disease control". In: *Proceedings of the Royal Society of London. Series B: Biological Sciences* 270.1533 (2003), pp. 2565–2571. DOI: 10.1098/rspb.2003.2554.

[Hel+20] Joel Hellewell, Sam Abbott, Amy Gimma, et al. "Feasibility of controlling 2019-nCoV outbreaks by isolation of cases and contacts". In: *The Lancet Global Health* 8.4 (Apr. 2020), pp. 488–496. DOI: 10.1101/2020.02.08.20021162.

[KTM] Max S. Kim, Stephania Taladrid, and Colin Marshall. *Seoul's Radical Experiment in Digital Contact Tracing*. URL: https://www.newyorker.com/news/news-desk/seouls-radical-experiment-in-digital-contact-tracing.

[20] *People Uncomfortable With Government Tracking, but Less So if It's to Fight Virus*. Mar. 2020. URL: https://morningconsult.com/2020/03/23/coronavirus-location-data-tracking/.

[Tha20] Ishaan Tharoor. *Analysis — Coronavirus kills its first democracy*. Mar. 2020. URL: https://www.washingtonpost.com/world/2020/03/31/coronavirus-kills-its-first-democracy/&sa=D&ust=1587947929298000&usg=AFQjCNESS35QMLSXNoq6L-NQXSsI5XUaIg.

[Ven20] Anand Venkatanarayanan. *Covid-19: How The Aarogya Setu App Handles Your Data*. Apr. 2020. URL: https://www.bloombergquint.com/coronavirus-outbreak/covid-19-how-the-aarogya-setu-app-handles-your-data.

[Jow19] Tom Jowitt. *Bluetooth 5.1 Delivers Pinpoint Location Accuracy: Silicon UK Tech News*. Nov. 2019. URL: https://www.silicon.co.uk/mobility/4g/bluetooth-5-1-location-accuracy-241087.

[Bay+20] Jason Bay, Joel Kek, Alvin Tan, et al. *BlueTrace: A privacy-preserving protocol forcommunity-driven contact tracing across borders*. 2020.

[Alt16] Alaa Althubaiti. "Information bias in health research: definition, pitfalls, and adjustment methods". In: *Journal of Multidisciplinary Healthcare* (2016), p. 211. DOI: 10.2147/jmdh.s104807.